21CS72

Model Question Paper-1 with effect from 2021 (CBCS Scheme)

USN □□□□□□□□□□

Seventh Semester B.E. Degree Examination

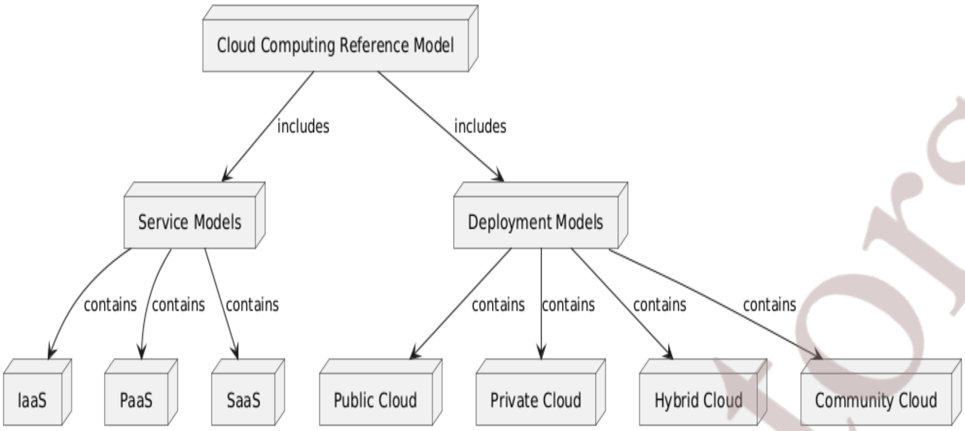
Subject Title: Cloud Computing

TIME: 03 Hours **Max. Marks: 100**

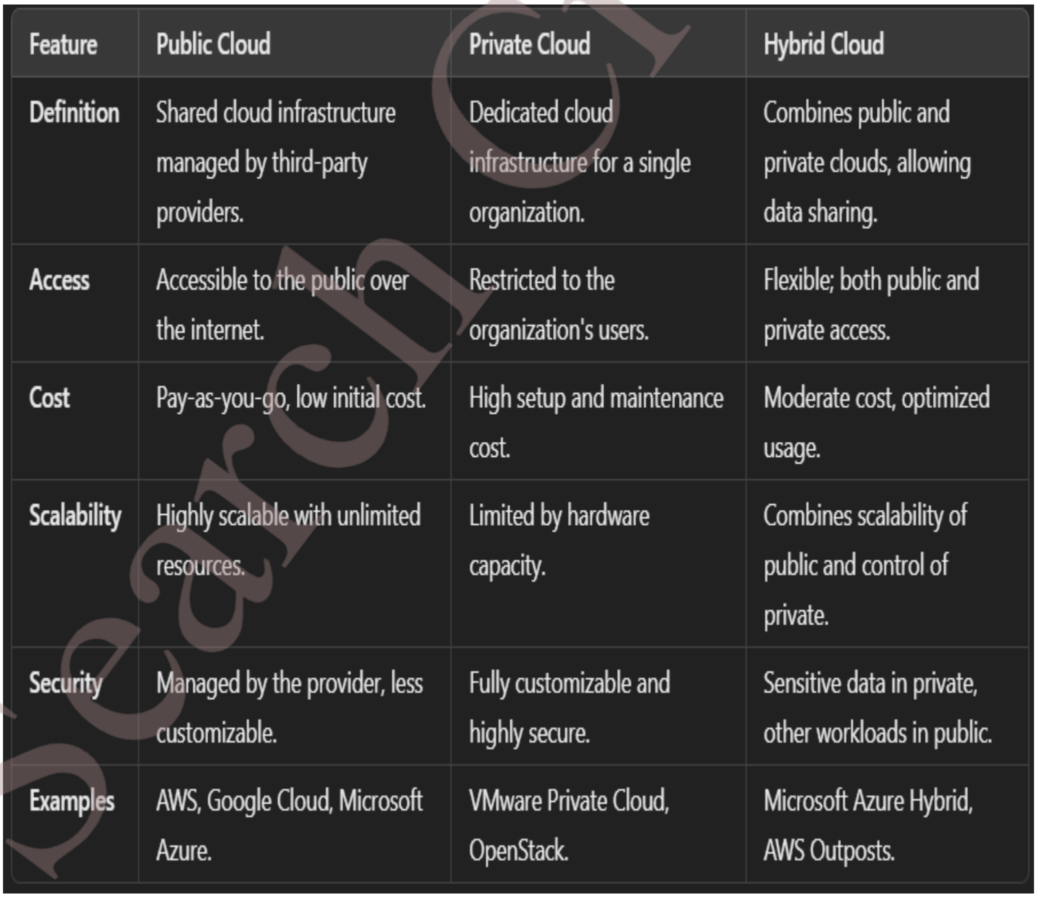
Note: 01. Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE**.

		Module -1	**COs**	**Marks**
Q.01	a	**Explain the cloud computing reference model with a neat diagram.** ➢ The Cloud Computing Reference Model is a framework that outlines the various services and deployment models in cloud computing. ➢ It provides a structured approach to understanding how cloud services are delivered and consumed. ➢ The model is generally divided into three primary service models and four deployment models. **Service Models** 1. **Infrastructure as a Service (IaaS):** o Provides virtualized resources such as storage, networks, and servers. o Example: Amazon EC2. 2. **Platform as a Service (PaaS):** o Offers a platform to build, test, and deploy applications. o Example: Google App Engine. 3. **Software as a Service (SaaS):** o Delivers software applications over the internet. o Example: Google Workspace. **Deployment Models** 1. **Public Cloud:** o Accessible to the public and owned by third-party providers. o Example: AWS.	1, 2	7

2. **Private Cloud:**
   - Dedicated for one organization with greater control and security.
   - Example: On-premises VMware cloud.
3. **Hybrid Cloud:**
   - Combines public and private clouds for flexibility.
   - Example: Azure Hybrid.
4. **Community Cloud:**
   - Shared infrastructure for organizations with common interests.
   - Example: Government clouds.



b **Explain the differences between public, private and hybrid cloud deployment models**.

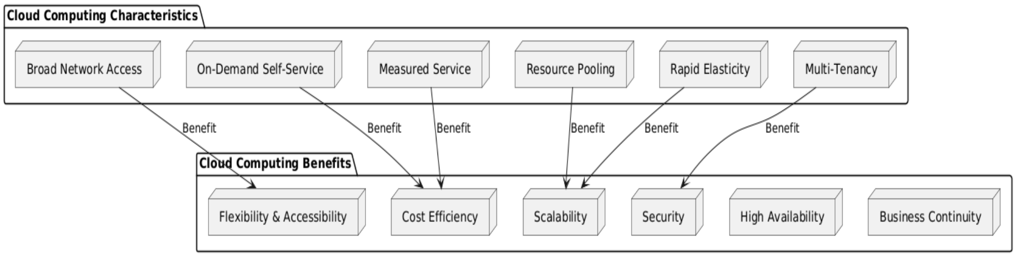


Feature	Public Cloud	Private Cloud	Hybrid Cloud
Definition	Shared cloud infrastructure managed by third-party providers.	Dedicated cloud infrastructure for a single organization.	Combines public and private clouds, allowing data sharing.
Access	Accessible to the public over the internet.	Restricted to the organization's users.	Flexible; both public and private access.
Cost	Pay-as-you-go, low initial cost.	High setup and maintenance cost.	Moderate cost, optimized usage.
Scalability	Highly scalable with unlimited resources.	Limited by hardware capacity.	Combines scalability of public and control of private.
Security	Managed by the provider, less customizable.	Fully customizable and highly secure.	Sensitive data in private, other workloads in public.
Examples	AWS, Google Cloud, Microsoft Azure.	VMware Private Cloud, OpenStack.	Microsoft Azure Hybrid, AWS Outposts.

1, 2

7

c **Elaborate the various cloud computing characteristics and its benefits.**



Cloud Computing Characteristics:

1. **On-Demand Self-Service:**
   - Users can provision computing resources (e.g., storage, processing power) without provider intervention.
2. **Broad Network Access:**
   - Services are accessible over the network (e.g., the internet) from a variety of devices.
3. **Resource Pooling:**
   - Cloud providers pool resources across multiple customers, ensuring efficient allocation based on demand.
4. **Rapid Elasticity:**
   - Cloud systems can scale resources up or down quickly based on workload demands.
5. **Measured Service:**
   - Resources are metered and billed based on usage, similar to utilities like electricity.
6. **Multi-Tenancy:**
   - Multiple users (tenants) share cloud infrastructure, with isolated data and processes.

Cloud Computing Benefits:

1. **Cost Efficiency:**
   - Reduces upfront infrastructure costs with a pay-as-you-go model.
2. **Scalability:**
   - Easily scale resources up or down based on user demand.
3. **Flexibility & Accessibility:**
   - Users can access services anytime and from anywhere with an internet connection.

1,2

6

		4. **Security:** ○ Providers implement advanced security features like encryption, authentication, and compliance with industry standards. 5. **High Availability:** ○ Cloud services provide high uptime, often backed by SLAs, ensuring minimal service disruption. 6. **Business Continuity:** ○ Disaster recovery and backup solutions ensure continuity during unforeseen events.		
OR				
Q.02	a	**List & Explain the various cloud computing platforms and technologies.** **1. Amazon Web Services (AWS)** - **On-Demand Compute & Storage**: Provides services like EC2 for compute power and S3 for scalable storage. - **Serverless Computing**: AWS Lambda allows running code without managing servers. - **Global Presence**: AWS has data centers across the globe for high availability and low latency. **2. Microsoft Azure** - **Hybrid Cloud Solutions**: Offers seamless integration between on-premises infrastructure and cloud. - **Compute and Storage**: Azure VMs for compute, Blob Storage for unstructured data. - **AI & Machine Learning**: Azure Cognitive Services enable AI capabilities for building intelligent applications. **3. Google Cloud Platform (GCP)** - **Big Data Analytics**: GCP offers BigQuery for fast, scalable analytics. - **Compute Engine**: Scalable virtual machines for applications. - **AI and ML**: GCP provides tools like TensorFlow and AutoML for machine learning projects. **4. IBM Cloud** - **Enterprise-Grade Solutions**: Focus on AI, blockchain, and IoT integrations.	1, 2	7

- **Kubernetes and Containers**: Managed Kubernetes for containerized applications.
- **Cloud Functions**: Serverless computing to automate tasks based on events.

5. Oracle Cloud

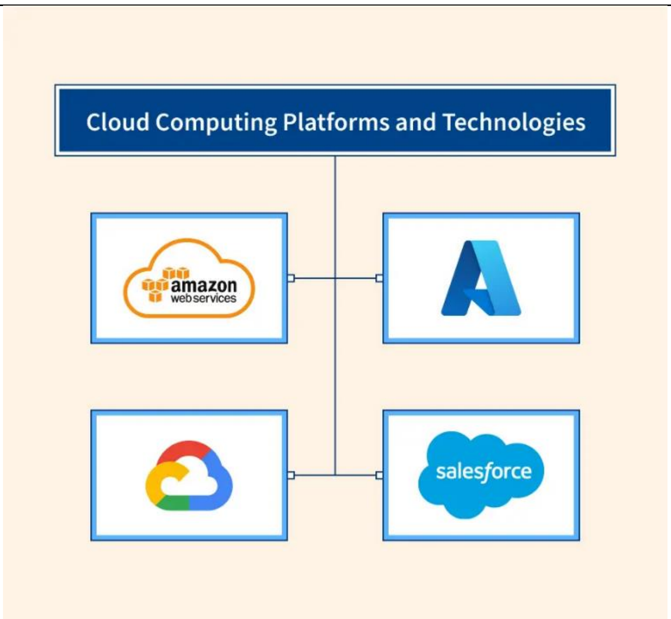
- **Autonomous Database**: Self-managing databases with integrated machine learning.
- **Enterprise Resource Planning (ERP)**: Oracle Cloud applications for finance, HR, and supply chain management.
- **Kubernetes Support**: Oracle Kubernetes Engine (OKE) for container orchestration.

6. Alibaba Cloud

- **Global Reach**: Especially strong in Asia-Pacific markets.
- **Elastic Compute Service (ECS)**: Virtual machines to run applications.
- **Big Data and AI**: Tools like MaxCompute and Machine Learning Platform for data processing and AI.

7. Cloud Technologies

- **Virtualization**: Enables running multiple virtual machines on a single physical host, crucial for efficient cloud operations.
- **Containers**: Tools like Docker and Kubernetes for easy application deployment and scaling.
- **Serverless**: Compute services like AWS Lambda that allow developers to run code without managing servers.
- **Microservices Architecture**: Cloud platforms support microservices for efficient, scalable application development.
- **Cloud Storage**: Services like AWS S3, Azure Blob Storage, and Google Cloud Storage for scalable data storage.
- **AI & ML Integration**: Most cloud platforms (e.g., GCP, Azure) offer tools to build, train, and deploy machine learning models.

		 Cloud Computing Platforms and Technologies amazon web services salesforce		
	b	**What are the major distributed computing technologies that led to cloud computing.** 1. **Virtualization** ○ Allows multiple virtual instances to run on a single physical machine by abstracting hardware resources. ○ Enables efficient resource utilization, scalability, and provisioning of virtual machines on-demand. 2. **Grid Computing** ○ Connects distributed systems to share computing resources for solving large-scale problems. ○ Demonstrates resource pooling and distributed computing, influencing cloud platforms to offer scalable, shared computing resources. 3. **Cluster Computing** ○ Uses interconnected machines (nodes) to work together as a single system to handle computational tasks. ○ Enables high-performance computing (HPC) and large-scale parallel processing, which is a key feature of cloud environments. 4. **Service-Oriented Architecture (SOA)** ○ Builds applications as modular, discrete services that can communicate over a network. ○ Lays the foundation for cloud service models like IaaS, PaaS, and SaaS.	1, 2	7

		5. **Peer-to-Peer (P2P) Networks** o Allows systems to share resources directly with one another without relying on a central server. o Promotes distributed resource sharing and decentralized computing, contributing to cloud's on-demand resource model. 6. **Parallel Computing** o Uses multiple processors or cores to perform tasks simultaneously. o Offers high-performance computing (HPC) for tasks requiring large-scale processing power. 7. **Distributed Databases** o Stores data across multiple locations and handles distributed queries and transactions. o Crucial for large-scale data storage, availability, and management in cloud services like AWS, Google Cloud, and Azure.		
	c	**Describe the main characteristics of a service-oriented computing.** **1. Loose Coupling** • Services are independent and communicate over well-defined interfaces. • This allows flexibility in service implementation, meaning changes can be made to one service without affecting others. **2. Interoperability** • SOC enables the interaction of different systems and platforms, regardless of the underlying technologies. • This is achieved through standardized communication protocols such as SOAP, REST, and XML. **3. Reusability** • Services are designed to be reusable across different applications and systems. • Once created, a service can be used multiple times by different consumers, reducing redundancy and improving efficiency. **4. Discoverability** • Services can be discovered and accessed dynamically through service registries. • This characteristic makes it easy to locate services and integrate them into new systems or applications.	1, 2	6

5. Modularity

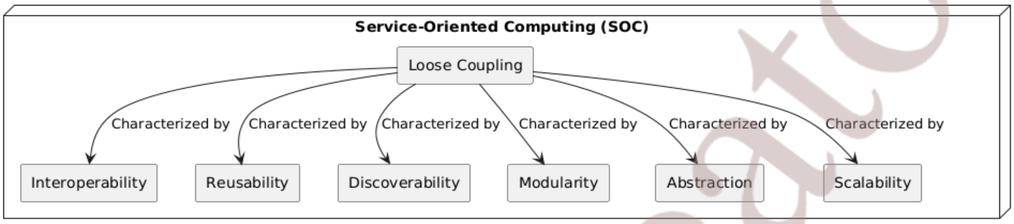
- Services are modular components, each performing a specific function.
- This modularity allows for easier maintenance, updates, and management of the system.

6. Abstraction

- Services abstract the underlying business logic, allowing clients to interact with high-level functionalities without needing to know the details of the implementation.
- This promotes simplicity and reduces complexity for service consumers.

7. Scalability

- SOC supports scaling both horizontally (adding more instances of services) and vertically (upgrading service capacity).
- It ensures that services can handle increased loads or expand with growing demands.



Module-2

Q. 03 a **Explain the characteristics of virtualized environments.**

1. Resource Pooling

- Virtualized environments pool physical resources (such as CPU, memory, and storage) and allocate them dynamically to virtual machines (VMs) based on demand.
- This allows for efficient use of hardware resources and flexibility in resource management.

2. Isolation

- Virtual machines (VMs) are isolated from each other and from the underlying hardware.
- This ensures that one VM's failure or issues do not impact others and helps maintain security and stability.

3. Flexibility and Scalability

- Virtualization enables the rapid creation, migration, and scaling of virtual machines without the need to reconfigure physical hardware.

2, 3 7

- New VMs can be created on-demand and allocated resources as needed, allowing the environment to scale with workload demands.

4. High Availability and Disaster Recovery

- Virtualized environments support features like live migration, snapshots, and failover mechanisms, ensuring high availability.
- In case of failure, VMs can be quickly restored from snapshots or migrated to another host, aiding disaster recovery.

5. Cost Efficiency

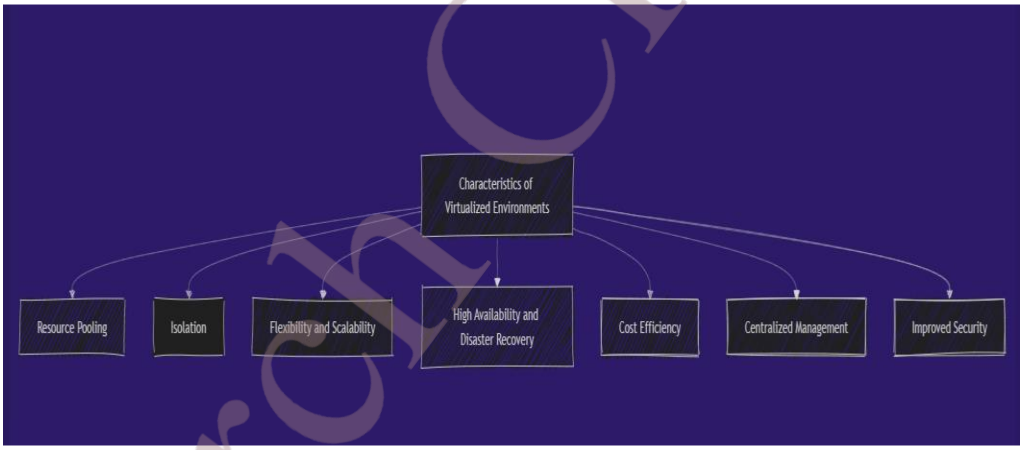
- Virtualization reduces the need for physical hardware by allowing multiple VMs to run on a single physical server.
- This results in lower hardware, maintenance, and energy costs, making it more cost-effective than traditional computing setups.

6. Centralized Management

- Virtualized environments allow for centralized management of VMs and physical resources through hypervisors and management software.
- This streamlines administrative tasks like resource allocation, monitoring, and maintenance.

7. Improved Security

- Each virtual machine operates independently, which enhances security by limiting the scope of attacks to individual VMs.
- Virtualized environments can implement security policies on a per-VM basis, providing more granular control over security measures.


Characteristics of Virtualized Environments
Resource Pooling
Isolation
Flexibility and Scalability
High Availability and Disaster Recovery
Cost Efficiency
Centralized Management
Improved Security

b **Give the taxonomy of virtualization techniques.** 2, 3 7

1. Hardware Virtualization

- **Definition**: Creates a virtual machine that simulates the physical hardware and runs an entire operating system (OS).
- **Techniques**: Hypervisor-based virtualization (Type 1 and Type 2 hypervisors).

- **Examples**: VMware, Microsoft Hyper-V, Xen.

2. Operating System Virtualization

- **Definition**: Virtualizes the operating system by allowing multiple isolated user-space instances (containers) on a single host OS.
- **Techniques**: Containerization and OS-level virtualization.
- **Examples**: Docker, LXC (Linux Containers), OpenVZ.

3. Network Virtualization

- **Definition**: Abstracts and splits the network resources into multiple virtual networks that can be independently controlled.
- **Techniques**: Virtual LANs (VLANs), software-defined networking (SDN), network function virtualization (NFV).
- **Examples**: Cisco ACI, VMware NSX.

4. Storage Virtualization

- **Definition**: Combines multiple physical storage devices into a single virtualized storage resource, improving management and efficiency.
- **Techniques**: Block-level and file-level virtualization.
- **Examples**: SAN (Storage Area Network), NAS (Network-Attached Storage), IBM Spectrum Virtualize.

5. Desktop Virtualization

- **Definition**: Allows for running desktop environments remotely, enabling centralized management and secure access.
- **Techniques**: Virtual Desktop Infrastructure (VDI), Remote Desktop Services (RDS).
- **Examples**: Citrix XenDesktop, VMware Horizon View.

6. Application Virtualization

- **Definition**: Runs applications in a virtual environment, isolating them from the underlying OS.
- **Techniques**: Application streaming, emulation.
- **Examples**: Microsoft App-V, VMware ThinApp.

7. Data Virtualization

- **Definition**: Provides a unified view of data from multiple sources without physically moving the data.
- **Techniques**: Data abstraction, real-time data access.
- **Examples**: Denodo, Red Hat JBoss Data Virtualization.

8. Process Virtualization

- **Definition**: Allows processes to run in isolated environments with abstracted system resources.
- **Techniques**: Process containers, resource control mechanisms.
- **Examples**: Docker, Kubernetes (for managing containers).

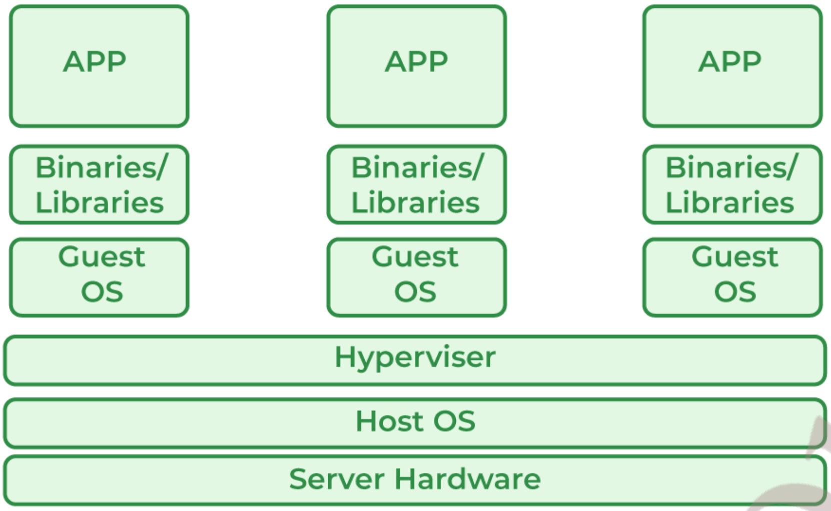
	c	**What is virtualization and what are its benefits.**	2, 3	6

1. Virtualization is the process of creating virtual versions of physical resources such as servers, storage, networks, and operating systems.
2. It allows multiple virtual environments (virtual machines or containers) to run on a single physical system, abstracting the hardware from the software.

Benefits of Virtualization

1. **Improved Resource Utilization**
   - Virtualization allows efficient use of hardware resources by running multiple virtual machines (VMs) on a single physical server.
2. **Cost Efficiency**
   - Reduces hardware costs by consolidating multiple physical machines into fewer servers, leading to savings in hardware, energy, and space.
3. **Increased Scalability and Flexibility**
   - Virtual machines can be created and scaled dynamically based on demand, providing flexibility for growing workloads.
4. **Simplified Management and Maintenance**
   - Centralized management tools make it easier to monitor, configure, and maintain virtual environments, streamlining administrative tasks.
5. **Enhanced Security**
   - VMs are isolated from each other, reducing the impact of failures or security breaches and improving overall system security.
6. **Disaster Recovery and High Availability**
   - Features like live migration, snapshots, and automated backups ensure high availability and facilitate quick recovery from failures.

7. **Faster Provisioning and Deployment**
   - Virtualization enables rapid provisioning of virtual machines, speeding up application deployment and time-to-market for new services.



Virtualization

OR

Q.04	a	**Explain virtualization and cloud computing and pros and cons of virtualization.**	2, 3	7

Virtualization

- Creates virtual instances of physical hardware resources like servers, storage, networks, or operating systems.
- Abstracts underlying hardware, allowing multiple virtual environments (VMs or containers) to run on a single physical machine.
- Each virtual environment operates independently, like a separate physical machine.

Cloud Computing

- Delivers computing services over the internet, including storage, processing power, networking, databases, software, etc.
- Services are provided by cloud providers like AWS, Microsoft Azure, and Google Cloud.
- Pay-as-you-go model with flexible, scalable resources without owning physical servers.

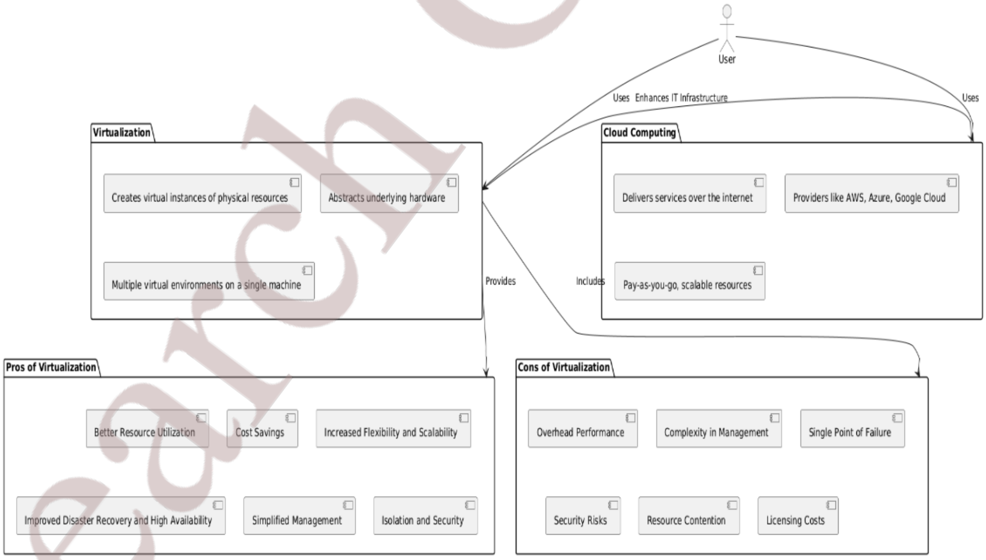
Pros of Virtualization

1. **Better Resource Utilization**: Optimizes physical hardware by running multiple VMs on a single host.

2. **Cost Savings**: Reduces the need for physical servers, saving on hardware, power, and space.
3. **Increased Flexibility and Scalability**: Allows virtual environments to be created, scaled, or resized based on demand.
4. **Improved Disaster Recovery and High Availability**: VMs can be easily migrated, cloned, or snapshotted for faster recovery and minimal downtime.
5. **Simplified Management**: Centralized tools make it easier to monitor and configure virtualized environments.
6. **Isolation and Security**: VMs are isolated from each other, preventing one failure or breach from affecting others.

Cons of Virtualization

1. **Overhead Performance**: Resource sharing between VMs can lead to performance degradation compared to running directly on physical hardware.
2. **Complexity in Management**: Managing a large number of VMs can become complex without the right tools.
3. **Single Point of Failure**: Host machine failure impacts all running VMs, leading to downtime.
4. **Security Risks**: Hypervisor vulnerabilities can cause security breaches across VMs.
5. **Resource Contention**: Sharing physical resources can result in performance issues.
6. **Licensing Costs**: Software licensing for multiple VMs can increase costs despite hardware savings.


User
Uses
Enhances IT Infrastructure
Uses
Virtualization
Creates virtual instances of physical resources
Abstracts underlying hardware
Multiple virtual environments on a single machine
Cloud Computing
Delivers services over the internet
Providers like AWS, Azure, Google Cloud
Pay-as-you-go, scalable resources
Provides
Includes
Pros of Virtualization
Better Resource Utilization
Cost Savings
Increased Flexibility and Scalability
Improved Disaster Recovery and High Availability
Simplified Management
Isolation and Security
Cons of Virtualization
Overhead Performance
Complexity in Management
Single Point of Failure
Security Risks
Resource Contention
Licensing Costs

	b	**Explain hypervisors and its types.**	2, 3	7

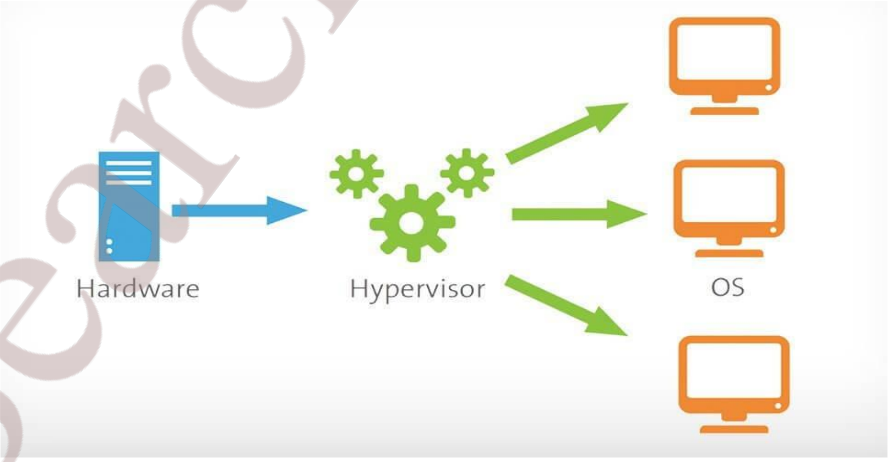
- A **hypervisor** is a software layer that allows multiple virtual machines (VMs) to run on a single physical machine.
- It abstracts the underlying hardware, enabling the creation, management, and isolation of virtual environments.
- The hypervisor controls the execution of virtual machines and ensures that each VM has its own dedicated resources while sharing the physical hardware.

Type 1 Hypervisor (Bare-metal Hypervisor)

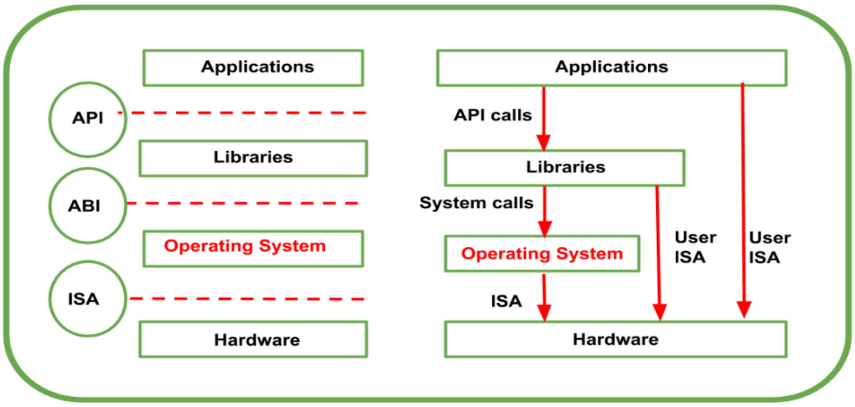
- Runs directly on the physical hardware of the host machine.
- No underlying operating system is required.
- Provides better performance by eliminating the need for an intermediary OS.
- More secure as it operates on bare-metal hardware with fewer attack vectors.
- More stable since it doesn't rely on an external OS.
- Used in data centers, enterprise environments, and production systems.
- Examples: VMware ESXi, Microsoft Hyper-V, Xen.

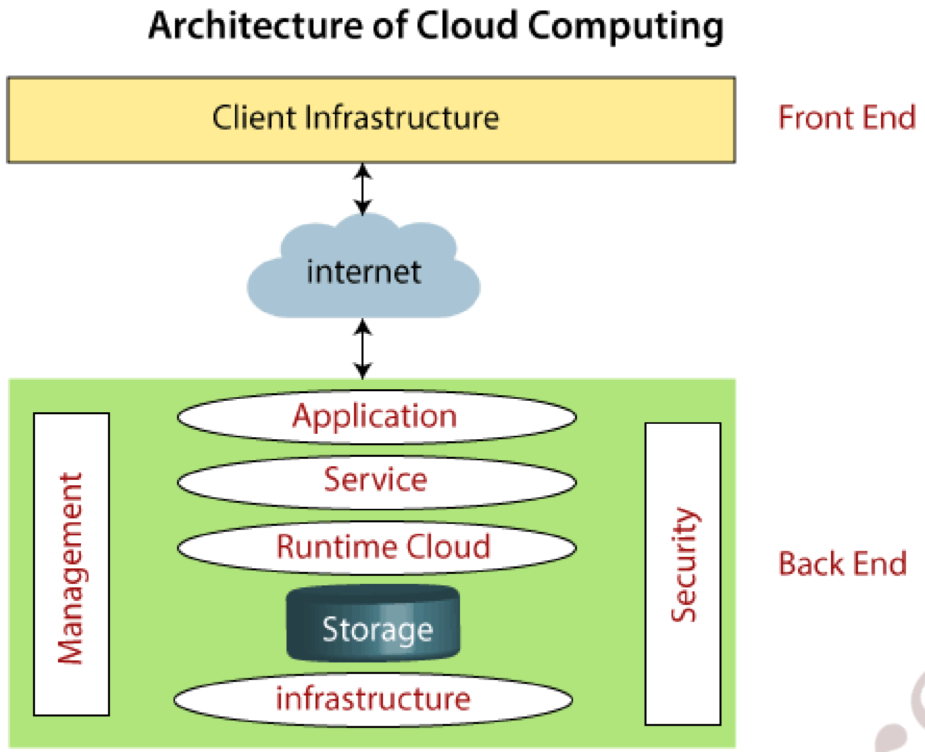
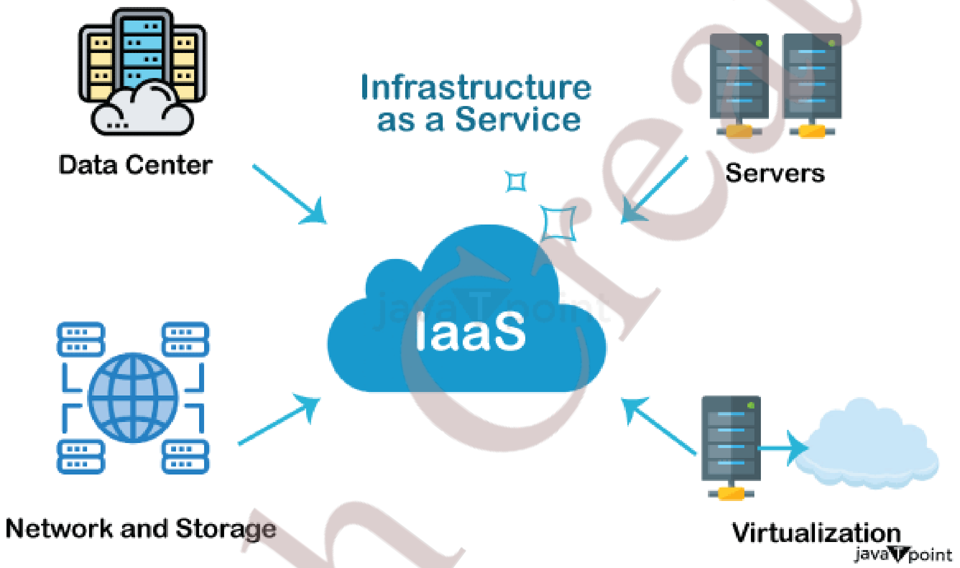
Type 2 Hypervisor (Hosted Hypervisor)

- Runs on top of an existing operating system (host OS).
- Relies on the host OS for resource management and operation.
- Easier to set up and use, making it suitable for personal use, development, and testing.
- Less efficient due to the additional layer of the host OS.
- More flexible as it can work on multiple operating systems.
- Used for development, testing, and non-production environments.
- Examples: VMware Workstation, Oracle VirtualBox, Parallels Desktop.



	c	**Discuss machine reference model of execution virtualization.** 1. **Physical Machine (PM)**: o The actual hardware that is being virtualized. o Includes processors, memory, storage, and network interfaces. 2. **Hypervisor/Virtual Machine Monitor (VMM)**: o Software layer that manages virtual machines. o Sits between the physical machine and the virtual machines to control access to resources. o Types: ▪ **Type 1 Hypervisor** (Bare-metal): Runs directly on the hardware. ▪ **Type 2 Hypervisor** (Hosted): Runs on top of a host OS. 3. **Virtual Machine (VM)**: o A virtualized environment that simulates a physical machine. o Each VM operates independently with its own virtual CPU, memory, storage, and network. 4. **Guest Operating System (OS)**: o OS running inside a virtual machine. o Can be different from the host OS and interacts with virtualized resources provided by the hypervisor. 5. **Virtualized Resources**: o Virtual components such as virtual CPUs, memory, storage, and network interfaces allocated to VMs by the hypervisor. o These resources are mapped from the physical hardware. 6. **How It Works**: o The hypervisor abstracts physical hardware and allocates resources to VMs. o Each VM runs a guest OS, which believes it has access to the physical hardware. o The hypervisor ensures resource allocation, isolation, and efficient utilization.	2, 3	6

		 Applications API Libraries ABI Operating System ISA Hardware Applications API calls Libraries System calls Operating System ISA User ISA User ISA Hardware		
Module-3				
Q. 05	a	**Briefly Explain cloud computing architecture with a neat diagram.** 1. **Front-End (Client Interface)** ○ Represents the user's device and application used to interact with the cloud. ○ Includes devices like PCs, smartphones, and tablets. ○ Uses browsers or specific software to access cloud services. 2. **Back-End (Cloud Service Provider Infrastructure)** ○ Contains all resources required to provide cloud services. ○ Components include: ▪ **Servers**: For data storage and processing. ▪ **Databases**: To store structured data. ▪ **Virtual Machines**: For scalability and efficiency. ▪ **Applications**: Hosted software services. ▪ **Security Mechanisms**: Protect data and ensure access control. 3. **Middleware** ○ Acts as a bridge between client-side applications and backend systems. ○ Ensures smooth communication and data management. 4. **Network** ○ Connects the front-end and back-end components. ○ Typically uses the Internet or a dedicated intranet. 5. **Security** ○ Firewalls, encryption, and identity management ensure secure transactions.	2, 3	7

		 Architecture of Cloud Computing Client Infrastructure Front End internet Management Application Service Runtime Cloud Storage infrastructure Security Back End		
	b	**Explain IAAS with a neat diagram.**  Data Center Infrastructure as a Service Servers IaaS Network and Storage Virtualization javaTpoint 1. Provides scalable computing resources like virtual servers and storage. 2. Users can deploy their operating systems, applications, and databases. 3. Offers on-demand resource provisioning with pay-as-you-go pricing. 4. Includes virtualized components like VMs, networks, and data storage. 5. Reduces dependency on physical infrastructure and hardware. 6. Enables automated resource management through APIs. 7. Supports disaster recovery and secure data backup. 8. Accessible via the internet from any compatible device.	2, 3	7
	c	**What is SAAS. Explain its characteristics and its initial benefits.**	2, 3	6

Software as a Service (SaaS)

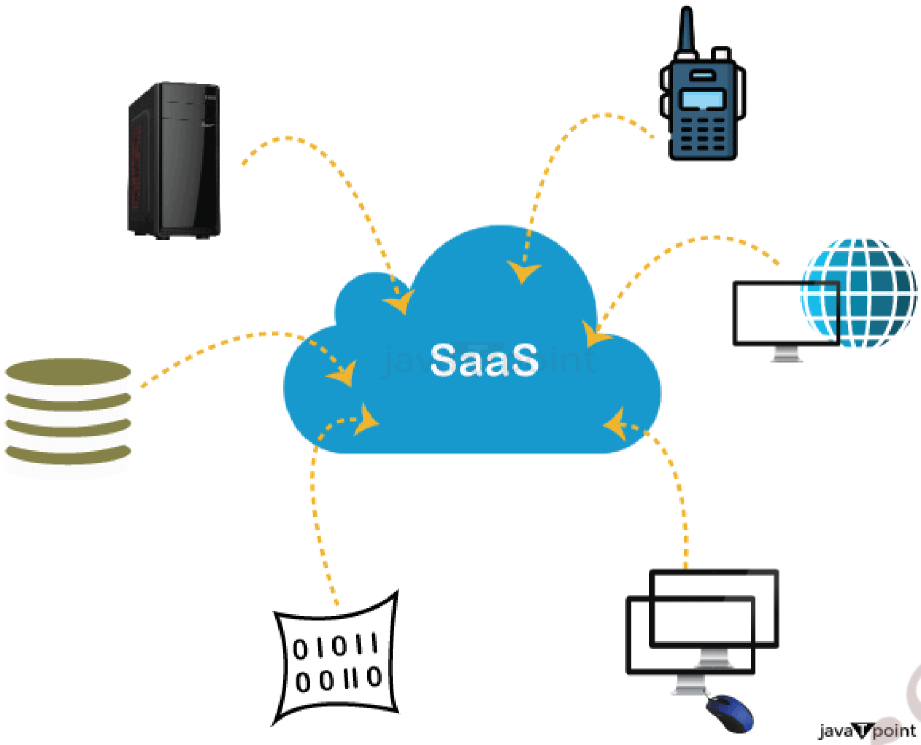
1. **Hosted Applications**: Software is hosted on cloud servers and managed by the provider.
2. **Internet Access**: Applications are accessed via a web browser using an internet connection.
3. **Subscription-Based**: Users pay based on a subscription model (monthly or annually).
4. **Automatic Updates**: Software updates and maintenance are handled by the provider.
5. **Scalable Usage**: Resources and services can be scaled up or down as per user needs.
6. **Multitenancy**: A single application instance serves multiple users.
7. **Device Independence**: Accessible on any device with a web browser.

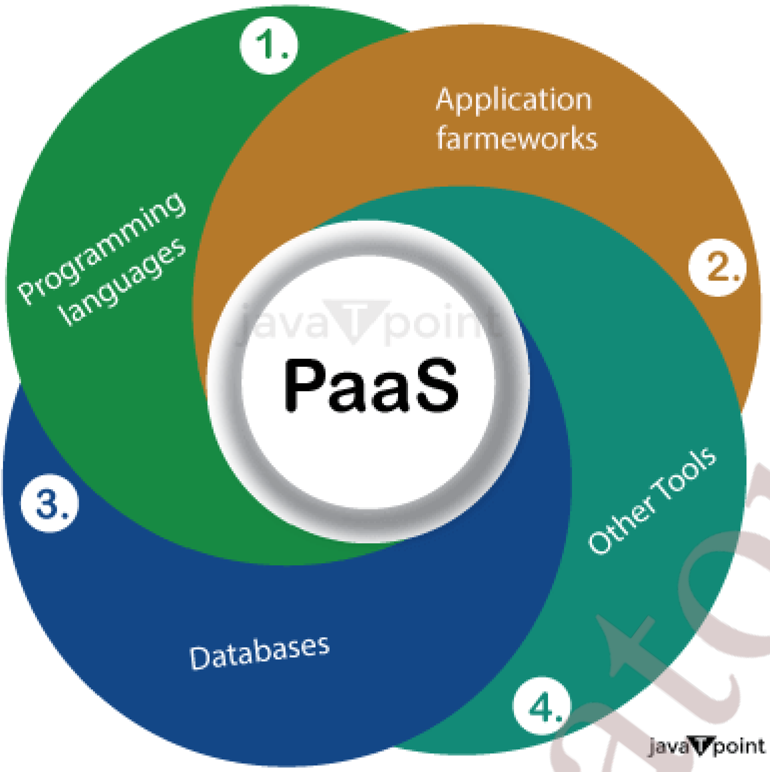
Characteristics of SaaS

1. **Web-Based Access**: Applications run directly from the browser without installation.
2. **Centralized Management**: Managed by the provider, ensuring consistent performance.
3. **Pay-As-You-Go**: Flexible pricing allows users to pay only for what they use.
4. **Global Accessibility**: Available anytime, anywhere with an internet connection.
5. **Seamless Integration**: Often integrates with other SaaS and third-party applications.

Initial Benefits of SaaS

1. **Cost Savings**: Reduces the need for upfront hardware and software investment.
2. **Quick Deployment**: Applications can be accessed immediately after subscription.
3. **Minimal Maintenance**: No responsibility for software updates or server management.
4. **Enhanced Collaboration**: Multiple users can work on the same application in real-time.
5. **Scalability**: Scales effortlessly with business requirements.
6. **User-Friendly**: Intuitive interfaces with minimal learning curves.

				
		OR		
Q. 06	a	**Explain PAAS with a neat diagram.** 1. **Cloud-Based Development**: Provides a cloud environment for developers to build, test, and deploy applications without managing infrastructure. 2. **Pre-Configured Tools**: Offers integrated development tools, libraries, and frameworks for coding, testing, and debugging applications. 3. **Managed Databases**: Includes databases that are automatically maintained and scaled. 4. **Middleware Services**: Includes essential services like messaging, authentication, and integration tools. 5. **Scalability**: Automatically adjusts resources based on the application's demand. 6. **Flexibility**: Supports various programming languages and development frameworks. 7. **Security**: Provides built-in security features for application protection. **Benefits of PaaS** 1. **Reduces Development Time**: Focus on coding while the platform handles infrastructure and environment setup. 2. **Cost-Effective**: No need to invest in or manage physical servers and hardware.	2, 3	7

		3. **Simplified Deployment**: Streamlines the process of deploying applications with pre-configured environments. 4. **Automatic Scaling**: Scales up or down based on the application's usage. 5. **Collaborative Development**: Facilitates team collaboration with cloud-based tools and shared environments.  1. Application farmeworks 2. Programming languages javaTpoint PaaS 3. Other Tools Databases 4. javaTpoint		
	b	**Describe the fundamental features of the economic and business model behind cloud computing.** 1. **Pay-as-You-Go (Usage-Based Pricing)** ○ Users pay for the resources they consume, such as storage, processing power, and bandwidth. ○ Flexible pricing eliminates upfront infrastructure costs. 2. **Cost Efficiency** ○ Reduces capital expenditures (CapEx) by shifting to operational expenditures (OpEx). ○ Cloud providers offer economies of scale, making services affordable for businesses. 3. **Scalability and Elasticity** ○ Resources can be scaled up or down based on demand. ○ Pay only for what is used, optimizing costs and managing cash flow. 4. **Subscription and Licensing Models**	2, 3	7

		○ Cloud services are typically provided through subscription-based models (e.g., SaaS, PaaS, IaaS). ○ Businesses subscribe to services based on their needs. 5. **Operational and Management Efficiency** ○ Providers handle infrastructure, maintenance, updates, security, and backups. ○ Businesses can focus on core activities instead of IT management. 6. **Global Accessibility and Collaboration** ○ Cloud services are accessible from anywhere with an internet connection. ○ Facilitates remote work, improving global collaboration and productivity. 7. **Business Continuity and Disaster Recovery** ○ Built-in disaster recovery and backup solutions ensure business continuity. ○ Data is replicated across locations for resilience and availability. 8. **Focus on Innovation** ○ Businesses can focus on innovation while cloud providers handle infrastructure. ○ Continuous service improvements from cloud providers. 9. **Market-Driven Pricing** ○ Competitive pricing among providers offers businesses multiple options. ○ Drives down prices and improves service offerings. 10. **Green Computing and Sustainability** ○ Providers invest in energy-efficient data centers and renewable energy. ○ Businesses benefit from reduced environmental impact.		
	c	**List and Explain some of the challenges in cloud computing.** 1. **Data Security and Privacy** ○ Storing sensitive information on the cloud introduces risks related to unauthorized access and data breaches. ○ Organizations must implement strong encryption, access controls, and comply with privacy regulations (e.g., GDPR, HIPAA) to safeguard data.	2, 3	6

2. **Downtime and Service Reliability**
   - Cloud services may experience outages or downtime due to hardware failures, cyberattacks, or natural disasters.
   - Downtime can disrupt business operations, and businesses must rely on Service Level Agreements (SLAs) to ensure high availability and reliability.
3. **Vendor Lock-In**
   - Migrating data and applications from one cloud provider to another can be complex due to different architectures, tools, and services.
   - Businesses may become dependent on a single cloud provider, which limits flexibility and can increase costs when switching vendors.
4. **Data Transfer and Bandwidth Costs**
   - Transferring large volumes of data to and from the cloud can incur substantial costs, especially when bandwidth is limited.
   - Ongoing data transfer can also slow down processes and increase operational costs, especially for data-intensive businesses.
5. **Compliance and Legal Issues**
   - Different regions have varying laws about data storage and privacy, complicating data management when using global cloud services.
   - Businesses must ensure compliance with specific regulations such as GDPR or industry-specific laws, requiring close monitoring of cloud provider practices.
6. **Limited Control and Flexibility**
   - Cloud users have limited control over the infrastructure, relying on the provider for updates, security patches, and resource allocation.
   - This lack of control may restrict customization and the ability to optimize resources or address specific business needs.

Module-4

Q. 07	a	**Explain operating system security and virtual machine security.**	3, 4	10

Operating System Security

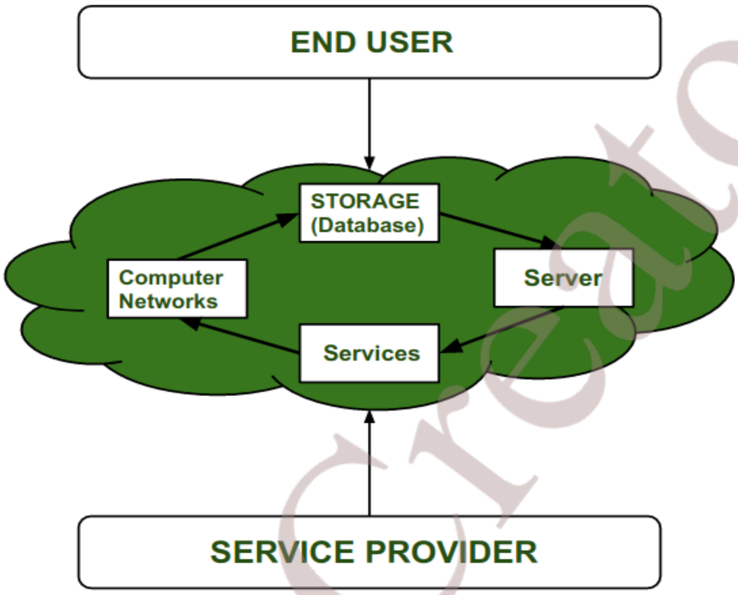
1. **User Authentication and Access Control**
   - Ensures that only authorized users can access the OS.
   - Methods: Passwords, biometrics, multi-factor authentication (MFA).

2. **Kernel Protection**
   - Protects the core of the OS from exploits and attacks.
   - Techniques: System call filtering, integrity checks, privilege separation.
3. **System Hardening**
   - Reduces vulnerabilities by disabling unused services and patching the OS.
   - Tools: Firewalls, Intrusion Detection Systems (IDS), and software updates.
4. **File System Security**
   - Secures files and directories from unauthorized access.
   - Uses: Access control lists (ACLs), encryption, file auditing.
5. **Malware Protection**
   - Protects the OS from malicious software (viruses, worms, ransomware).
   - Tools: Antivirus software, sandboxing, and behavior analysis.
6. **Network Security**
   - Secures communication and protects from network-based attacks.
   - Tools: SSL/TLS, IPsec, firewalls, VPNs.
7. **Privilege Management**
   - Ensures users and applications are granted the least privilege.
   - Tools: Role-based access control (RBAC), access control lists (ACLs).
8. **Auditing and Monitoring**
   - Tracks user actions and system activities for suspicious behavior.
   - Tools: Logging, SIEM (Security Information and Event Management) systems.
9. **Patch Management**
   - Keeps the system up to date by applying security patches.
   - Tools: Automatic patching, update managers.
10. **Backup and Recovery**

- Ensures data can be recovered in case of disaster.
- Techniques: Regular backups, disaster recovery plans.

Virtual Machine Security

1. **Isolation and Segmentation**
   - Ensures VMs are isolated to prevent attacks from spreading.
   - Tools: Hypervisor, virtual network segmentation.
2. **Hypervisor Security**
   - Protects the hypervisor, which manages the VMs, from attacks.
   - Techniques: Hypervisor patching, minimizing attack surface, secure boot.
3. **VM Encryption**
   - Encrypts VM disks and memory to protect data confidentiality.
   - Tools: Full disk encryption, memory encryption.
4. **Access Control**
   - Restricts unauthorized access to VMs and their management interface.
   - Techniques: Role-based access control (RBAC), multi-factor authentication.
5. **VM Integrity and Configuration Management**
   - Monitors the integrity of VMs and their configurations.
   - Tools: Integrity verification, configuration management tools (e.g., Chef, Puppet).
6. **Live Migration Security**
   - Ensures the secure transfer of VMs between physical hosts.
   - Techniques: Secure protocols, encrypted VM migration.
7. **Resource Allocation and Monitoring**
   - Prevents denial-of-service (DoS) by ensuring fair resource allocation.
   - Tools: Resource monitoring, anomaly detection systems.

		8. **Patch Management** ○ Ensures VMs and hypervisors are up to date with security patches. ○ Tools: Automated patching tools for VM and hypervisor security. 9. **Monitoring and Intrusion Detection** ○ Continuously monitors for suspicious activities or potential attacks. ○ Tools: Intrusion detection systems (IDS), network monitoring. 10. **Backup and Disaster Recovery** ○ Protects against VM data loss or failures by maintaining backups. ○ Techniques: Regular VM snapshots, disaster recovery plans.		
	b	**Explain the security risks posed by shared images and management os.**  END USER STORAGE (Database) Computer Networks Server Services SERVICE PROVIDER **Security Risks Posed by Shared Images:** 1. **Malicious Code Injection**: ○ Shared images can be pre-configured with malicious software that might go undetected during the creation or deployment of the image. When other users deploy the image, they might unknowingly execute this malicious code. 2. **Unpatched Vulnerabilities**: ○ If the shared image is not updated regularly, it may contain outdated software with known vulnerabilities. This exposes the system to exploits and attacks.	3, 4	10

3. **Data Leakage**:
   - Sensitive data stored in a shared image may be accessible to other users or systems using the image. Improper data handling within shared images can lead to unauthorized data access.
4. **Privilege Escalation**:
   - Shared images might contain embedded administrator or root privileges. If the image is not securely configured, it can allow unauthorized users to escalate their privileges and gain control of the system.
5. **Lack of Isolation**:
   - In some cases, shared images may not have proper isolation between different users or virtual machines. This can lead to unintentional access to data or resources belonging to other users.
6. **Compliance and Legal Risks**:
   - Shared images may not meet the required security and privacy standards for regulated industries. This poses a risk of non-compliance with laws such as GDPR, HIPAA, or PCI-DSS.
7. **Insecure Configuration**:
   - Misconfigured settings in a shared image could lead to weak security controls, allowing attackers to exploit weaknesses in the system.
8. **Inadequate Monitoring**:
   - Without adequate monitoring, it becomes difficult to detect suspicious activities related to shared images, such as unauthorized access or malicious activity.

Security Risks Posed by Management Operating Systems (OS):

1. **Privilege Escalation and Unauthorized Access**:
   - If an attacker gains control of the management OS, they can escalate privileges and gain access to all virtual machines and systems managed by the OS. This can result in total control over the infrastructure.
2. **Weak Authentication and Access Control**:
   - A poorly implemented authentication mechanism or lack of proper access control allows unauthorized users to access the management OS, putting all virtual environments at risk.

3. **Denial of Service (DoS) Attacks**:
    - A compromised management OS can be used to perform DoS attacks on the virtual machines or containers, causing outages or performance degradation across all hosted services.
4. **Insecure Communication**:
    - Communication between the management OS and other systems, such as virtual machines, could be intercepted if unencrypted protocols are used. This could expose sensitive data or allow attackers to tamper with communication.
5. **Inadequate Resource Management**:
    - Poor resource allocation and management in the management OS can allow malicious users or processes to consume excessive system resources, leading to degraded performance or system crashes.
6. **Exposure of Management Interfaces**:
    - The management OS often exposes interfaces for managing virtual machines or containers. If these interfaces are not secured, attackers may exploit them to compromise the system.
7. **Unpatched Vulnerabilities**:
    - The management OS may contain vulnerabilities that can be exploited by attackers if not properly patched. This makes the OS a prime target for security breaches.
8. **Insider Threats**:
    - Employees or individuals with access to the management OS may intentionally or unintentionally cause damage, leak data, or compromise system security.
9. **Misconfigurations**:
    - Misconfigurations in the management OS can lead to vulnerabilities, including incorrect user permissions, weak passwords, or incorrect networking settings, all of which increase the risk of exploitation.
10. **Lack of Auditing and Monitoring**:

- Without proper logging and monitoring, it becomes difficult to detect unusual activities or potential security breaches in the management OS, leaving the system vulnerable to attacks.

OR

Q. 08	a	**Explain the concept of privacy impact assessment and its importance in cloud computing.** 1. Privacy Impact Assessment (PIA) is a process to evaluate the effects of data handling practices on individuals' privacy, identifying and mitigating privacy risks in cloud environments where personal data is processed. 2. The main aim of PIA is to assess privacy risks, ensure compliance with privacy laws, and protect personal data. It helps organizations understand the impact of their data handling practices on privacy and put measures in place to secure it. 3. PIA involves assessing what personal data is collected, how it is processed, where it is stored, how it is shared, and how long it will be retained or disposed of, ensuring the entire data lifecycle is considered. 4. PIA helps identify potential privacy risks such as unauthorized access, data leakage, and improper sharing of personal information, which could lead to breaches or violations of privacy laws. 5. It ensures that organizations comply with legal regulations such as GDPR, HIPAA, and CCPA by confirming that personal data is managed according to legal standards for data protection, transfer, and storage. 6. PIA enhances transparency by documenting how personal data is handled and processed, ensuring accountability in managing user data and addressing concerns from users or regulatory bodies. 7. Conducting a PIA builds user trust by demonstrating that the cloud service provider is committed to protecting personal data, encouraging users to trust the service and feel secure about their information. 8. PIA promotes data minimization, ensuring that only necessary data is collected and processed. This reduces the risks associated with data breaches and limits exposure to sensitive information. 9. PIA helps enhance security measures by identifying weaknesses and recommending improvements, such as encryption, secure data transmission, and access control, to prevent unauthorized access. 10. PIA supports the principle of "Privacy by Design" by integrating privacy measures into the design and architecture of cloud systems from the beginning, helping reduce privacy risks in the development and deployment stages.	3, 4	10

	b	**Explain the following associated with cloud computing** **i) cloud security risks** **ii) Security: the top concern for cloud users.**	3, 4	10

i) Cloud Security Risks

1. **Data Breaches**: Sensitive data stored in the cloud can be targeted by cybercriminals, leading to unauthorized access and exposure.
2. **Data Loss**: Cloud service failures, such as hardware malfunctions or data corruption, can result in permanent loss of data.
3. **Insider Threats**: Authorized individuals within the organization may misuse their access to compromise data security, either intentionally or unintentionally.
4. **Lack of Visibility and Control**: Cloud users may not have full visibility into the cloud infrastructure, limiting their control over security measures.
5. **Insecure APIs**: Vulnerabilities in cloud service APIs can provide attackers with opportunities to gain unauthorized access.
6. **Inadequate Data Encryption**: Without proper encryption of data at rest and during transit, sensitive information is vulnerable to interception or breaches.
7. **Account Hijacking**: Attackers can gain unauthorized access to user accounts through methods like phishing or weak passwords, leading to data theft or destruction.
8. **Shared Technology Vulnerabilities**: Multi-tenant cloud environments expose users to potential risks due to shared infrastructure that could affect the security of multiple tenants.
9. **Denial of Service (DoS) Attacks**: Cloud services are susceptible to DoS or DDoS attacks that can overwhelm resources, causing outages or disruptions.
10. **Compliance and Legal Issues**: Failure to comply with data protection regulations like GDPR or HIPAA can result in legal consequences and penalties.

ii) Security: The Top Concern for Cloud Users

1. **Loss of Control Over Data**: Cloud users often have limited control over their data, raising concerns about its safety and accessibility.
2. **Trust in Cloud Providers**: Security depends on the cloud provider’s infrastructure, creating a reliance on their practices and the potential risk of mismanagement.
3. **Complexity of Security Measures**: Implementing and maintaining cloud security measures, such as encryption and access control, requires expertise, which may be challenging for users.

4. **Lack of Transparency**: Many cloud providers offer limited insight into their security measures, making it hard for users to fully assess security risks.
5. **Multi-Tenant Architecture**: Sharing infrastructure with other users increases the risk of data leakage or unauthorized access if security isn't properly maintained.
6. **Changing Regulatory Landscape**: Different countries have varying regulations on data privacy, which may complicate security management for cloud users.
7. **Increased Attack Surface**: Cloud services, being distributed across various systems, create more potential points of attack for cybercriminals.
8. **Dependence on Cloud Providers' Security Measures**: Users rely on cloud providers for certain security aspects, such as physical security and network protection, but are responsible for their own security practices as well.
9. **Data Sovereignty**: Cloud users may face issues related to where their data is stored, as different countries have specific laws governing data access and transfer.
10. **Cost of Security Failures**: Security incidents in the cloud can lead to high costs in terms of recovery, penalties, and loss of reputation, making security a critical investment.

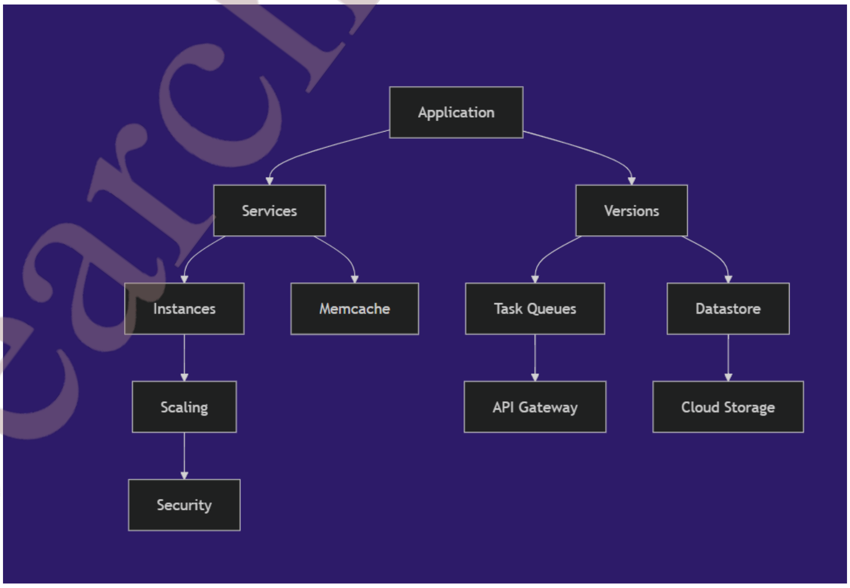
Module-5

Q. 09	a	**Explain the core components of Google app engine.**	3, 4	10

Core Components of Google App Engine

1. **Application**:
   - The code and files that make up the web application or service.
   - Uploaded and managed on Google App Engine.
2. **Services**:
   - Divides the application into different parts (e.g., front-end, back-end).
   - Each service can be scaled independently.
3. **Versions**:
   - Multiple versions of services can run simultaneously.
   - Allows gradual feature rollout, testing, and rollback.
4. **Instances**:
   - Virtual machines (VMs) running the application.
   - Automatically scaled based on traffic and resource requirements.
5. **Datastore**:
   - A NoSQL database used for storing application data.
   - Supports high availability, transactions, and efficient queries.

6. **Task Queues**:
    - Manages background jobs asynchronously.
    - Allows tasks like sending emails or processing images to be handled later.
7. **Memcache**:
    - A distributed caching system to store frequently accessed data in memory.
    - Improves performance by reducing database load.
8. **API Gateway**:
    - Manages access to the application's APIs.
    - Controls routing, authentication, and traffic for APIs.
9. **Cloud Storage**:
    - Provides scalable storage for unstructured data like images and videos.
    - Integrated with Google Cloud for durable, high-availability storage.
10. **App Engine SDK**:
    - Tools and libraries for building and testing applications locally.
    - Includes a local development server and command-line tools.
11. **Scaling**:
    - Automatically adjusts the number of instances based on incoming traffic.
    - Ensures performance during high traffic and scales down during low traffic.
12. **Security**:
    - Built-in security features like IAM, SSL/TLS encryption, and integration with Google Cloud security tools.
    - Allows controlling access and securing resources.



	b	**Discuss in detail the following media applications of cloud computing technologies.** **i) Animoto** **ii) Maya Rendering with Aneka** **iii) Video encoding on cloud.**	3, 4	10

Media Applications of Cloud Computing Technologies:

i) Animoto:

- **Cloud-Based Video Creation**: Allows users to create professional videos from photos, video clips, and music using cloud resources.
- **Cloud Rendering**: Offloads video processing and rendering to the cloud, saving local computing power.
- **Scalability**: Cloud infrastructure scales based on user demand, ensuring optimal performance during high traffic.
- **Cost Efficiency**: Cloud resources reduce the need for powerful local hardware, lowering overall production costs.
- **Collaboration**: Multiple users can work together on video projects from different locations.
- **Accessibility**: Available globally, enabling users to create and edit videos from anywhere with an internet connection.

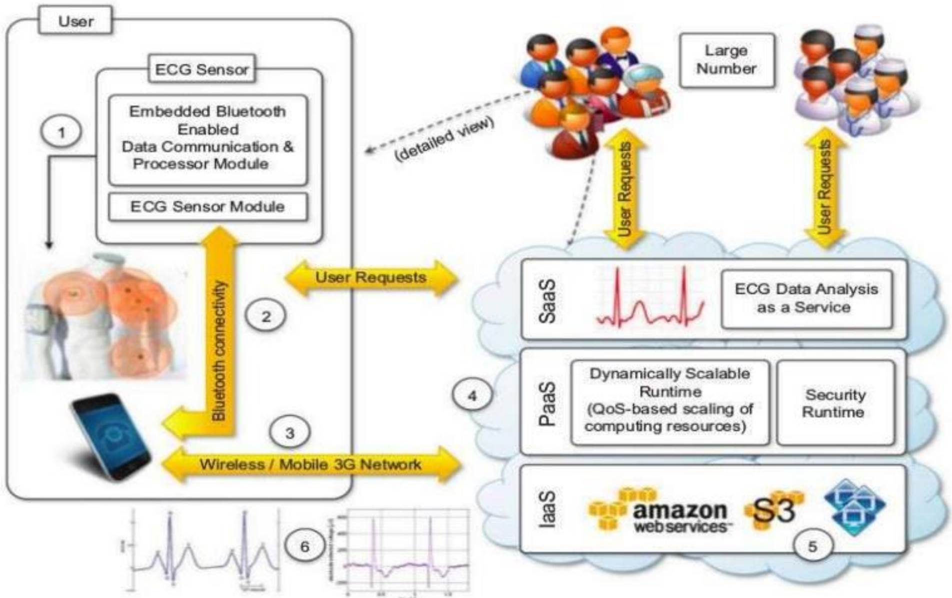
ii) Maya Rendering with Aneka:

- **Distributed Rendering**: Distributes rendering tasks across multiple cloud resources, significantly speeding up the process.
- **Elastic Resource Allocation**: Resources like processing power and storage are dynamically allocated to match the workload.
- **Scalability**: Cloud infrastructure scales rendering capabilities based on the complexity and volume of the animation.
- **Cost Efficiency**: By utilizing a pay-per-use model for cloud resources, users can avoid the capital cost of dedicated hardware.
- **Faster Rendering**: Cloud-based rendering reduces the time required to process complex 3D animations.
- **High-Performance Computing**: Leverages the power of cloud servers for intensive rendering tasks, delivering high-quality outputs quickly.

iii) Video Encoding on Cloud:

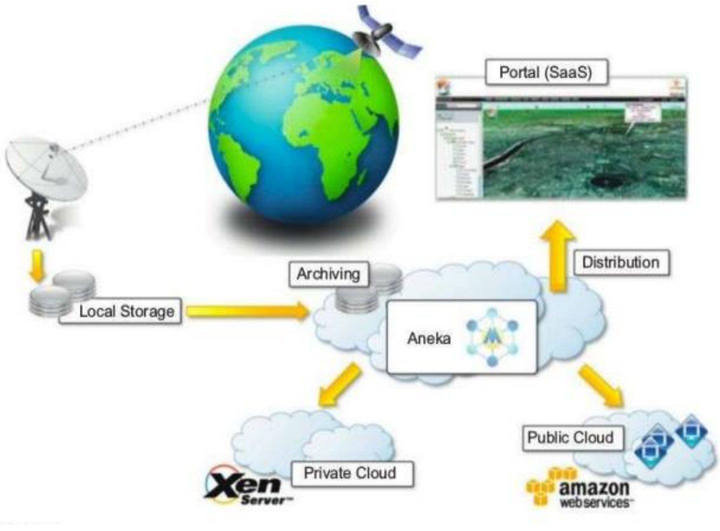
- **Scalable Encoding**: Cloud services scale resources to handle large volumes of video data for encoding.
- **Parallel Processing**: Multiple cloud servers process video encoding tasks simultaneously, speeding up the encoding process.

		- **Multiple Formats Support**: Supports encoding into various formats (e.g., MP4, MOV, AVI) and resolutions to meet diverse device requirements. - **Global Accessibility**: Enables users to access and encode videos from anywhere in the world. - **Efficient Content Delivery**: Integrated with CDNs for faster distribution of encoded videos across global networks. - **Cost-Effective**: Pay-as-you-go model reduces costs by only charging for the resources used during the encoding process.		
OR				
Q. 10	a	**Explain in detail about the application of cloud computing in** **i) Healthcare: ECG analysis in the cloud** **ii) Geoscience: satellite image processing** **i) Healthcare: ECG Analysis in the Cloud** 1. **Data Storage and Access**: Cloud provides secure, scalable storage for ECG data, making it accessible from anywhere. 2. **Real-Time Monitoring and Analysis**: ECG data can be monitored and analyzed instantly on the cloud, allowing immediate alerts for abnormalities. 3. **Scalability**: Cloud infrastructure can scale based on the volume of ECG data, offering more resources when needed. 4. **Data Security and Compliance**: Cloud services ensure data privacy and comply with healthcare standards like HIPAA, using encryption and access controls. 5. **Integration with Other Health Data**: ECG data can be integrated with other health records (patient history, test results) for a comprehensive analysis. 6. **Collaboration and Telemedicine**: Enables collaboration between healthcare providers worldwide and supports telemedicine for remote diagnosis. 7. **Cost Efficiency**: Reduces the need for expensive on-premise hardware for ECG storage and processing. 8. **Cloud-Based Machine Learning**: Machine learning algorithms can be used on cloud resources to analyze ECG data for detecting conditions like arrhythmia.	3, 4	10


User
ECG Sensor
Embedded Bluetooth Enabled Data Communication & Processor Module
ECG Sensor Module
1
2
3
4
5
6
Bluetooth connectivity
User Requests
Wireless / Mobile 3G Network
(detailed view)
Large Number
User Requests
User Requests
SaaS
ECG Data Analysis as a Service
PaaS
Dynamically Scalable Runtime (QoS-based scaling of computing resources)
Security Runtime
IaaS
amazon web services
S3

ii) Geoscience: Satellite Image Processing

1. **Data Storage and Management**: Cloud offers scalable storage for large satellite images, making them easily accessible and manageable.
2. **High-Performance Computing**: Cloud provides high computational power for processing complex satellite images quickly.
3. **Scalability**: Resources can be scaled up or down depending on the size and complexity of satellite images being processed.
4. **Parallel Processing**: Cloud platforms allow parallel processing of satellite images, improving speed and efficiency.
5. **Big Data Analytics**: Cloud systems can handle large volumes of geospatial data and apply analytics for insights such as detecting environmental changes.
6. **Collaboration and Sharing**: Satellite data and analysis can be shared easily among global teams for better collaboration.
7. **Machine Learning Integration**: Cloud can use machine learning algorithms to automatically analyze and detect patterns or anomalies in satellite imagery.
8. **Real-Time Analysis**: Cloud allows real-time processing of satellite data for applications like disaster management or environmental monitoring.
9. **Cost Efficiency**: Reduces costs by offering on-demand resources without the need for expensive infrastructure.
10. **Disaster Management**: Cloud-based satellite image processing helps in rapid damage assessment, mapping disaster areas, and coordinating response efforts.



	b	**Explain Amazon web services (AWS) in detail.**	3, 4	10

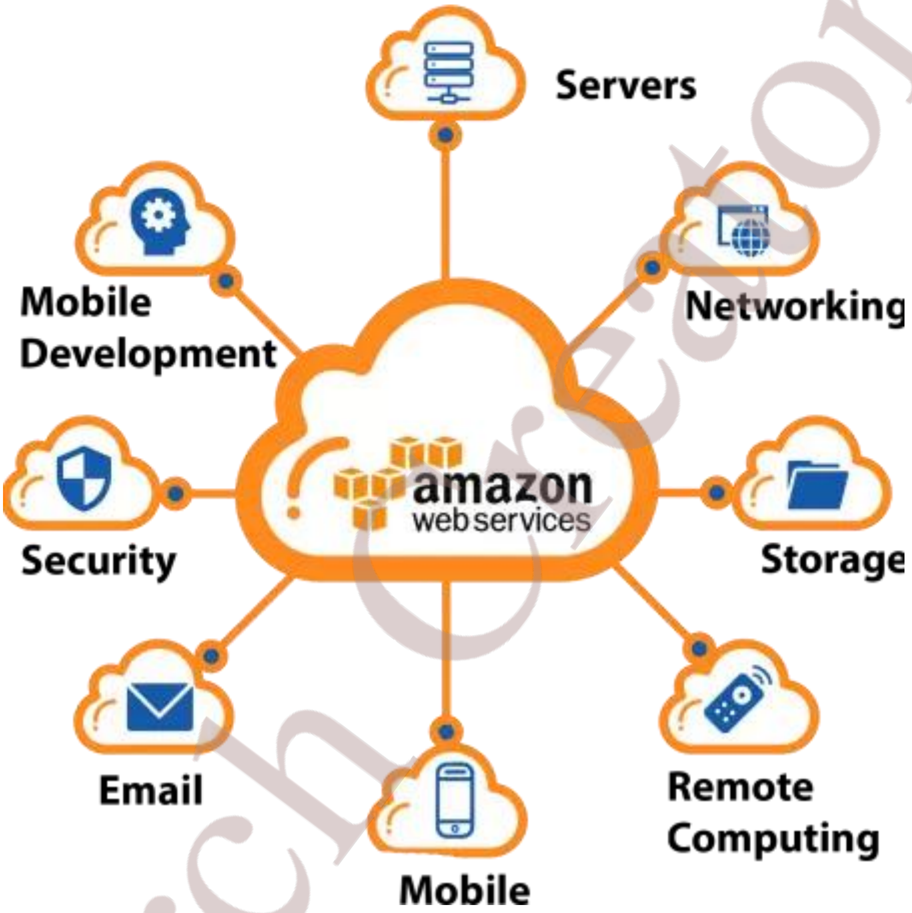
Amazon Web Services (AWS)

1. **Overview**:
   - AWS is a cloud computing platform provided by Amazon, offering a wide range of services such as computing power, storage, networking, databases, and machine learning.
2. **Core Services**:
   - **Compute**:
     - **Amazon EC2 (Elastic Compute Cloud)**: Scalable virtual servers for running applications.
     - **AWS Lambda**: Serverless computing to run code in response to events.
     - **Amazon Lightsail**: Simplified virtual private servers.
   - **Storage**:
     - **Amazon S3**: Object storage for backups, content delivery, and big data.
     - **Amazon EBS**: Persistent block-level storage for EC2 instances.
     - **Amazon Glacier**: Long-term data storage at lower costs.
   - **Networking**:
     - **Amazon VPC (Virtual Private Cloud)**: Isolated networks for secure communication between resources.
     - **Amazon Route 53**: DNS service for routing traffic.
     - **Elastic Load Balancing**: Distributes incoming traffic across EC2 instances for high availability.

   - **Databases**:
     - **Amazon RDS**: Managed relational database service.
     - **Amazon DynamoDB**: Managed NoSQL database service.
     - **Amazon Redshift**: Managed data warehousing for big data analytics.

3. **Machine Learning & AI**:
   - **Amazon SageMaker**: Platform for building, training, and deploying machine learning models.
   - **Amazon Rekognition**: Image and video analysis using deep learning.
   - **Amazon Polly**: Converts text to lifelike speech.
   - **AWS Deep Learning AMIs**: Pre-configured images for deep learning tasks.
4. **Security**:
   - **AWS IAM (Identity and Access Management)**: Manages user permissions and access.
   - **AWS Shield**: DDoS protection service.
   - **AWS WAF (Web Application Firewall)**: Protects applications from common web exploits.
5. **Developer Tools**:
   - **AWS CodeCommit**: Managed Git repositories for source code.
   - **AWS CodePipeline**: Continuous integration and delivery service.
   - **AWS CodeDeploy**: Automates deployment of applications to compute resources.
   - **AWS Cloud9**: Cloud-based integrated development environment (IDE).
6. **Analytics**:
   - **Amazon EMR (Elastic MapReduce)**: Managed Hadoop framework for processing large datasets.
   - **AWS Kinesis**: Real-time data streaming and analytics service.
   - **Amazon QuickSight**: Business intelligence service for data visualization.
7. **Cloud Management Tools**:
   - **AWS CloudWatch**: Monitoring service for AWS resources and applications.
   - **AWS CloudTrail**: Tracks user activity and API usage for security auditing.
   - **AWS Cost Explorer**: Tracks AWS usage and costs.

8. **Benefits of AWS**:
   - **Scalability**: Easily scale resources up or down based on demand.
   - **Cost-Effectiveness**: Pay only for the resources used with a pay-as-you-go model.
   - **Reliability**: High availability and fault tolerance with multiple availability zones.
   - **Security**: Strong encryption, IAM, and compliance with industry standards.
   - **Global Reach**: Data centers across the globe ensure low-latency access and disaster recovery.
   - **Innovation**: Frequent updates and new service offerings for cutting-edge technologies.


Servers
Mobile Development
Networking
amazon web services
Security
Storage
Email
Remote Computing
Mobile